

Andrew G. Gunem, No. 354042
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
T: (872) 263-1100
F: (872) 263-1109
agunem@straussborrelli.com

Attorneys for Plaintiff and Proposed Class

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION**

ANGEL JIMENEZ, on behalf of himself and
all others similarly situated,

Plaintiff,

v.

AMERIT FLEET SOLUTIONS, INC.,

Defendant.

Case No.

**CLASS ACTION COMPLAINT
FOR DAMAGES, INJUNCTIVE
RELIEF, AND EQUITABLE
RELIEF FOR:**

- 1. NEGLIGENCE;**
- 2. NEGLIGENCE *PER SE*;**
- 3. BREACH OF IMPLIED
CONTRACT;**
- 4. INVASION OF PRIVACY;**
- 5. UNJUST ENRICHMENT;**
- 6. BREACH OF FIDUCIARY
DUTY;**
- 7. CALIFORNIA UNFAIR
COMPETITION LAW;**
- 8. CALIFORNIA CONSUMER
PRIVACY ACT;**
- 9. DECLARATORY JUDGMENT.**

DEMAND FOR JURY TRIAL

Angel Jimenez (“Plaintiff”), through his attorneys, individually and on behalf of all others
similarly situated, brings this Class Action Complaint against Defendant Amerit Fleet Solutions,
Inc. (“Amerit” or “Defendant”), and its present, former, or future direct and indirect parent

1 companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the
2 following on information and belief—except as to his own actions, counsel’s investigations, and
3 facts of public record.

4 NATURE OF ACTION

5 1. This class action arises from Defendant’s failure to protect highly sensitive data.

6 2. Defendant provides “nationwide fleet maintenance” services to “7 of the 10 largest
7 fleets in the country[.]”¹ To that end, Defendant employs “technicians, fleet managers, garage
8 support, and account managers[.]”²

9 3. As such, Defendant stores a litany of highly sensitive personal identifiable
10 information (“PII”) and protected health information (“PHI”)—together “PII/PHI”—about its
11 current and former employees. But Defendant lost control over that data when cybercriminals
12 infiltrated its insufficiently protected computer systems in a data breach (the “Data Breach”).

13 4. It is unknown for precisely how long the cybercriminals had access to Defendant’s
14 network before the breach was discovered. In other words, Defendant had no effective means to
15 prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals
16 unrestricted access to its current and former employees’ PII/PHI.

17 5. On information and belief, cybercriminals were able to breach Defendant’s
18 systems because Defendant failed to adequately train its employees on cybersecurity and failed
19 to maintain reasonable security safeguards or protocols to protect the Class’s PII/PHI. In short,
20 Defendant’s failures placed the Class’s PII/PHI in a vulnerable position—rendering them easy
21 targets for cybercriminals.

22 6. Plaintiff is a Data Breach victim, having received a breach notice—attached as
23 Exhibit A. He brings this class action on behalf of himself, and all others harmed by Defendant’s
24 misconduct.

25
26 ¹ *Services*, AMERIT, <https://www.ameritfleetsolutions.com/services/> (last visited May 28, 2024).

27 ² *Id.*

7. The exposure of one's PII/PHI to cybercriminals is a bell that cannot be unrung. Before this data breach, its current and former employees' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

8. Plaintiff, Angel Jimenez, is a natural person and citizen of California. He resides in Fontana, California where he intends to remain.

9. Defendant, Amerit Fleet Solutions, Inc., is a General Stock Corporation incorporated in California and with its principal place of business at 1333 N. California Boulevard, Walnut Creek, California 94596.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. Members of the proposed Class are citizens of different states than Defendant. And there are over 100 putative Class members.

11. This Court has personal jurisdiction over Defendant because it is headquartered in California, regularly conducts business in California, and has sufficient minimum contacts in California.

12. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII/PHI of Plaintiff and the Class

13. Defendant provides "nationwide fleet maintenance" services to "7 of the 10 largest fleets in the country[.]"³ To that end, Defendant employs "technicians, fleet managers, garage support, and account managers[.]"⁴

³ *Services*, AMERIT, <https://www.ameritfleetsolutions.com/services/> (last visited May 28, 2024).

⁴ *Id.*

14. As part of its business, Defendant receives and maintains the PII/PHI of thousands of its current and former employees.

15. In collecting and maintaining the PII/PHI, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their PII/PHI.

16. Under state and federal law, businesses like Defendant have duties to protect its current and former employees' PII/PHI and to notify them about breaches.

17. Defendant recognizes these duties, declaring in its "Privacy Policy" that:

- a. "The security of your Personal Information is important to AFS."⁵
- b. "Any Personal Information that you provide AFS may be used to contact or identify you but is not subject to third parties or outside sources."⁶
- c. "AFS will not identify you to outside sources[.]"⁷
- d. "[W]e strive to use commercially acceptable means to protect your Personal Information[.]"⁸

Defendant's Data Breach

18. On January 21, 2024, Defendant realized that it was hacked in the Data Breach.⁹

19. Worryingly, Defendant has already admitted that "certain files were copied from its systems by an unauthorized person[.]"¹⁰

⁵ *Privacy Policy*, AMERIT, <https://www.ameritfleetsolutions.com/privacy-policy/> (last visited May 28, 2024).

⁶ *Id.*

⁷ *Id.*

⁸ *Id.*

⁹ *Data Breach Notification*, MAINE ATTY GEN, <https://apps.web.maine.gov/online/aeviewer/ME/40/d3991df2-5605-46cf-847a-b69aa01cfc54.shtml> (last visited May 28, 2024).

¹⁰ *Id.*

20. Still, Defendant has been unable to determine when the Data Breach began—explaining only that PII/PHI was stolen “likely in the January timeframe[.]”¹¹ Thus, upon information and belief, the Data Breach began prior to January 2024.

21. Because of Defendant’s Data Breach, at least the following types of PII/PHI were compromised:

- a. names;
- b. Social Security numbers;
- c. driver’s license information;
- d. financial account information; and
- e. medical information.¹²

22. In total, Defendant injured at least 1,912 persons—via the exposure of their PII/PHI—in the Data Breach.¹³ Upon information and belief, these 1,912 persons include its current and former employees.

23. And yet, Defendant waited over until April 26, 2024, before it began notifying the class—a full 96 days after the Data Breach was discovered.¹⁴

24. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

25. And when Defendant did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiff and the Class:

- a. “remain vigilant against instances of identity theft and fraud by reviewing your account statements;”
- b. “place a ‘credit freeze’ on a credit report;”

¹¹ *Id.*

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.*

1 c. “educate [yourself] regarding identity theft, fraud alerts, credit freezes, and
2 the steps [you] can take to protect your personal information by contacting
3 the consumer reporting bureaus, the Federal Trade Commission, or [your]
4 state Attorney General.”¹⁵

5 26. Defendant failed its duties when its inadequate security practices caused the Data
6 Breach. In other words, Defendant’s negligence is evidenced by its failure to prevent the Data
7 Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendant caused
8 widespread injury and monetary damages.

9 27. Since the breach, Defendant has promised to be “working to enhance its existing
10 security safeguards.”¹⁶ But this is too little too late. Simply put, these measures—which
11 Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

12 28. On information and belief, Defendant failed to adequately train its employees on
13 reasonable cybersecurity protocols or implement reasonable security measures.

14 29. Further, the Notice of Data Breach shows that Defendant cannot—or will not—
15 determine the full scope of the Data Breach, as Defendant has been unable to determine precisely
16 what information was stolen and when.

17 30. Defendant has done little to remedy its Data Breach. True, Defendant has offered
18 some victims credit monitoring and identity related services. But upon information and belief,
19 such services are wholly insufficient to compensate Plaintiff and Class members for the injuries
20 that Defendant inflicted upon them.

21 31. Because of Defendant’s Data Breach, the sensitive PII/PHI of Plaintiff and Class
22 members was placed into the hands of cybercriminals—inflicting numerous injuries and
23 significant damages upon Plaintiff and Class members.

24
25
26 ¹⁵ *Id.*

27 ¹⁶ *Id.*

32. Worryingly, this Data Breach appears to be part and parcel of Defendant's *pattern of negligent data security*. For example, back in 2022, an employee of Defendant reported on "Indeed" that:

- a. "personal information security is not taken seriously;" and
- b. "My I9 form was lost multiple times then shared on unsecure avenues with other employees who should not have had access to such personal information."¹⁷

Amerit Fleet Solutions

Amerit Fleet Solutions Vendor fleet manager Review

2.0

☆☆☆☆

Highly disorganized and no personal information security

Vendor fleet manager (Former Employee) - Remote - July 31, 2022

As a vendor fleet manager you will have unrealistic goals, no support and be the middle man between outside vendors looking for past due payments with no time frame to provide for when Amerit will pay. Amerit does not honor there payments terms nor do they have an accounts payable team in place to handle the large amount of incoming invoices they have every day. As a vendor fleet manager you will do very little in regards to fleet management and primarily be tasked with invoicing which is not mentioned in the job descriptions at all. They expect you to work 14-15 hour days vs hiring the appropriate number of people needed fit the job. On top of these issues personal information security is not taken seriously. My I9 form was lost multiple times then shared on unsecure avenues with other employees who should not have had access to such personal information. Also I was paying for insurance for 6 months and at the end of my employment found out that there insurance provider was not accepted in my state. They did eventually provide a refund but even that took some doing. Overall can not recommend this company

✗ Cons

Management/hr

¹⁷ *Amerit Fleet Solutions: Highly disorganized and no personal information security*, INDEED, (July 21, 2022) <https://www.indeed.com/cmp/Amerit-Fleet-Solutions/reviews/highly-disorganized-and-no-personal-information-security?id=0c187bf44dfd0a69>.

33. Moreover, upon information and belief, the cybercriminals in question are particularly sophisticated. After all, the cybercriminals: (1) defeated the relevant data security systems, (2) gained actual access to sensitive data, and (3) successfully “copied” files.¹⁸

34. And as the Harvard Business Review notes, such “[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking.”¹⁹

35. Thus, on information and belief, Plaintiff’s and the Class’s stolen PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

Plaintiff’s Experiences and Injuries

36. Plaintiff Angel Jimenez is a former employee of Defendant—having worked for Defendant for approximately one year in or around 2023.

37. Thus, Defendant obtained and maintained Plaintiff’s PII/PHI.

38. As a result, Plaintiff was injured by Defendant’s Data Breach.

39. As a condition of his employment with Defendant, Plaintiff provided Defendant with his PII/PHI. Defendant used that PII/PHI to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII/PHI in order to obtain employment and payment for that employment.

40. Plaintiff provided his PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant’s internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff’s PII/PHI and has a

¹⁸ *Data Breach Notification*, MAINE ATTY GEN, <https://apps.web.maine.gov/online/aewviewer/ME/40/d3991df2-5605-46cf-847a-b69aa01cfc54.shtml> (last visited May 28, 2024).

¹⁹ Brenda R. Sharton, *Your Company’s Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) <https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back>.

1 continuing legal duty and obligation to protect that PII/PHI from unauthorized access and
2 disclosure.

3 41. Plaintiff reasonably understood that a portion of the funds paid to Defendant
4 (and/or derived from his employment) would be used to pay for adequate cybersecurity and
5 protection of PII/PHI.

6 42. Plaintiff does not recall ever learning that his information was compromised in a
7 data breach incident—other than the breach at issue here.

8 43. Plaintiff received a Notice of Data Breach in early May 2024.

9 44. Thus, on information and belief, Plaintiff's PII/PHI has already been published—
10 or will be published imminently—by cybercriminals on the Dark Web.

11 45. Through its Data Breach, Defendant compromised at least Plaintiff's:

- 12 a. name;
- 13 b. date of birth;
- 14 c. driver's license information;
- 15 d. state identification information; and
- 16 e. Social Security number.

17 46. Plaintiff has *already* suffered from identity theft and fraud, including:

- 18 a. Plaintiff received approximately forty (40) emails regarding different
19 fraudulent loan and/or credit applications that were made in his name;
- 20 b. fraudulent charges of approximately \$900 were placed on a credit account
21 in Plaintiff's name through Credit One Bank (Plaintiff did not place these
22 charges nor create this account);
- 23 c. an unrecognized phone number was connected to Plaintiff's IRS tax
24 account (Plaintiff discovered this when he attempted to file his taxes);

25 47. Moreover, Plaintiff later learned that the fraudulent credit account with Credit One
26 Bank was added to his official credit report.

1 48. Thereafter, in the fallout of this substantial identity theft and fraud, Plaintiff's
2 credit score plummeted by approximately 30 points.

3 49. Plaintiff has spent five (5) hours attempting to mitigate the fallout of the Data
4 Breach, including, *inter alia*,

- 5 a. reviewing his accounts for further identity theft and fraud;
- 6 b. communicating with the IRS regarding the unrecognized phone number;
- 7 and
- 8 c. verifying his identity through a virtual meeting with an IRS agent.

9 50. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in
10 spam and scam phone calls and emails.

11 51. Plaintiff fears for his personal financial security and worries about what
12 information was exposed in the Data Breach.

13 52. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to
14 suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond
15 allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of
16 injuries that the law contemplates and addresses.

17 53. Plaintiff suffered actual injury from the exposure and theft of his PII/PHI—which
18 violates his rights to privacy.

19 54. Plaintiff suffered actual injury in the form of damages to and diminution in the
20 value of his PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant
21 was required to adequately protect.

22 55. Plaintiff suffered imminent and impending injury arising from the substantially
23 increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed
24 Plaintiff's PII/PHI right in the hands of criminals.

25 56. Because of the Data Breach, Plaintiff anticipates spending considerable amounts
26 of time and money to try and mitigate his injuries.

57. Today, Plaintiff has a continuing interest in ensuring that his PII/PHI—which, upon information and belief, remains backed up in Defendant’s possession—is protected and safeguarded from additional breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

58. Because of Defendant’s failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

- a. loss of the opportunity to control how their PII/PHI is used;
- b. diminution in value of their PII/PHI;
- c. compromise and continuing publication of their PII/PHI;
- d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;
- e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;
- f. delay in receipt of tax refund monies;
- g. unauthorized use of their stolen PII/PHI; and
- h. continued risk to their PII/PHI—which remains in Defendant’s possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII/PHI.

59. Stolen PII/PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII/PHI can be worth up to \$1,000.00 depending on the type of information obtained.

60. The value of Plaintiff and Class’s PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the “Dark Web”—further exposing the information.

61. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII/PHI far and wide.

62. One way that criminals profit from stolen PII/PHI is by creating comprehensive dossiers on individuals called “Fullz” packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII/PHI, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

63. The development of “Fullz” packages means that the PII/PHI exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

64. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class members’ stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

65. Defendant disclosed the PII/PHI of Plaintiff and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII/PHI of Plaintiff and Class members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII/PHI.

66. Defendant’s failure to promptly and properly notify Plaintiff and Class members of the Data Breach exacerbated Plaintiff and Class members’ injury by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

67. Defendant’s data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

68. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.²⁰

69. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”²¹

70. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant’s industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

71. According to the Federal Trade Commission (“FTC”), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

72. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.²² The FTC declared that, *inter alia*, businesses must:

- a. protect the personal customer information that they keep;

²⁰ See 2021 Data Breach Annual Report, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) <https://notified.idtheftcenter.org/s/>.

²¹ Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware>.

²² *Protecting Personal Information: A Guide for Business*, FED TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

- b. properly dispose of personal information that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand their network's vulnerabilities; and
- e. implement policies to correct security problems.

73. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

74. Furthermore, the FTC explains that companies must:

- a. not maintain information longer than is needed to authorize a transaction;
- b. limit access to sensitive data;
- c. require complex passwords to be used on networks;
- d. use industry-tested methods for security;
- e. monitor for suspicious activity on the network; and
- f. verify that third-party service providers use reasonable security measures.

75. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

76. In short, Defendant’s failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former employees’ data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

77. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-

malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

78. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

79. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

80. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

Defendant Violated HIPAA

81. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.²³

²³ HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

1 82. HIPAA provides specific privacy rules that require comprehensive administrative,
2 physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI
3 and PHI is properly maintained.²⁴

4 83. The Data Breach itself resulted from a combination of inadequacies showing
5 Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures
6 include, but are not limited to:

- 7 a. failing to ensure the confidentiality and integrity of electronic PHI that it
8 creates, receives, maintains and transmits in violation of 45 C.F.R. §
9 164.306(a)(1);
- 10 b. failing to protect against any reasonably-anticipated threats or hazards to
11 the security or integrity of electronic PHI in violation of 45 C.F.R. §
12 164.306(a)(2);
- 13 c. failing to protect against any reasonably anticipated uses or disclosures of
14 electronic PHI that are not permitted under the privacy rules regarding
15 individually identifiable health information in violation of 45 C.F.R. §
16 164.306(a)(3);
- 17 d. failing to ensure compliance with HIPAA security standards by
18 Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);
- 19 e. failing to implement technical policies and procedures for electronic
20 information systems that maintain electronic PHI to allow access only to
21 those persons or software programs that have been granted access rights in
22 violation of 45 C.F.R. § 164.312(a)(1);
- 23 f. failing to implement policies and procedures to prevent, detect, contain and
24 correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

25
26 ²⁴ See 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308
27 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312
28 (technical safeguards).

- g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);
- h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and
- i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

84. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

85. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

All individuals residing in the United States whose PII/PHI was compromised in the Data Breach discovered by Amerit in January 2024, including all those individuals who received notice of the breach.

86. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

87. Plaintiff reserves the right to amend the class definition.

88. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

1 89. Ascertainability. All members of the proposed Class are readily ascertainable from
2 information in Defendant's custody and control. After all, Defendant already identified some
3 individuals and sent them data breach notices.

4 90. Numerosity. The Class members are so numerous that joinder of all Class
5 members is impracticable. Upon information and belief, the proposed Class includes at least 1,912
6 members.

7 91. Typicality. Plaintiff's claims are typical of Class members' claims as each arises
8 from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable
9 manner of notifying individuals about the Data Breach.

10 92. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's
11 common interests. His interests do not conflict with Class members' interests. And Plaintiff has
12 retained counsel—including lead counsel—that is experienced in complex class action litigation
13 and data privacy to prosecute this action on the Class's behalf.

14 93. Commonality and Predominance. Plaintiff's and the Class's claims raise
15 predominantly common fact and legal questions—which predominate over any questions
16 affecting individual Class members—for which a class wide proceeding can answer for all Class
17 members. In fact, a class wide proceeding is necessary to answer the following questions:

- 18 a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's
19 and the Class's PII/PHI;
- 20 b. if Defendant failed to implement and maintain reasonable security
21 procedures and practices appropriate to the nature and scope of the
22 information compromised in the Data Breach;
- 23 c. if Defendant were negligent in maintaining, protecting, and securing
24 PII/PHI;
- 25 d. if Defendant breached contract promises to safeguard Plaintiff and the
26 Class's PII/PHI;
- 27
- 28

- e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;
- f. if Defendant's Breach Notice was reasonable;
- g. if the Data Breach caused Plaintiff and the Class injuries;
- h. what the proper damages measure is; and
- i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

94. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

95. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

96. Plaintiff and the Class entrusted their PII/PHI to Defendant on the premise and with the understanding that Defendant would safeguard their PII/PHI, use their PII/PHI for business purposes only, and/or not disclose their PII/PHI to unauthorized third parties.

97. Defendant owed a duty of care to Plaintiff and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry

standards for data security—would compromise their PII/PHI in a data breach. And here, that foreseeable danger came to pass.

98. Defendant has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiff and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

99. Defendant owed these duties to Plaintiff and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff and Class members' PII/PHI.

100. Defendant owed—to Plaintiff and Class members—at least the following duties to:

- a. exercise reasonable care in handling and using the PII/PHI in its care and custody;
- b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;
- c. promptly detect attempts at unauthorized access;
- d. notify Plaintiff and Class members within a reasonable timeframe of any breach to the security of their PII/PHI.

101. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

102. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII/PHI it was no longer required to retain under applicable regulations.

103. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII/PHI of Plaintiff and the Class involved an

1 unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the
2 criminal acts of a third party.

3 104. Defendant's duty to use reasonable security measures arose because of the special
4 relationship that existed between Defendant and Plaintiff and the Class. That special relationship
5 arose because Plaintiff and the Class entrusted Defendant with their confidential PII/PHI, a
6 necessary part of obtaining services from Defendant.

7 105. The risk that unauthorized persons would attempt to gain access to the PII/PHI and
8 misuse it was foreseeable. Given that Defendant hold vast amounts of PII/PHI, it was inevitable
9 that unauthorized individuals would attempt to access Defendant's databases containing the
10 PII/PHI—whether by malware or otherwise.

11 106. PII/PHI is highly valuable, and Defendant knew, or should have known, the risk
12 in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiff and Class members'
13 and the importance of exercising reasonable care in handling it.

14 107. Defendant improperly and inadequately safeguarded the PII/PHI of Plaintiff and
15 the Class in deviation of standard industry rules, regulations, and practices at the time of the Data
16 Breach.

17 108. Defendant breached these duties as evidenced by the Data Breach.

18 109. Defendant acted with wanton and reckless disregard for the security and
19 confidentiality of Plaintiff's and Class members' PII/PHI by:

- 20 a. disclosing and providing access to this information to third parties and
21 b. failing to properly supervise both the way the PII/PHI was stored, used,
22 and exchanged, and those in its employ who were responsible for making
23 that happen.

24 110. Defendant breached its duties by failing to exercise reasonable care in supervising
25 its agents, contractors, vendors, and suppliers, and in handling and securing the personal
26 information and PII/PHI of Plaintiff and Class members which actually and proximately caused
27 the Data Breach and Plaintiff and Class members' injury.

111. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class members' injuries-in-fact.

112. Defendant has admitted that the PII/PHI of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

113. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

114. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

115. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiff and the Class)

116. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

117. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII/PHI.

118. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such

as Defendant, of failing to use reasonable measures to protect the PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class members' sensitive PII/PHI.

119. Defendant breached its respective duties to Plaintiff and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII/PHI.

120. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

121. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

122. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiff and Class members would not have been injured.

123. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII/PHI.

124. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiff's and Class members' PHI.

125. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PHI that

1 Defendant collected and stored and the foreseeable consequences of a data breach, including,
2 specifically, the immense damages that would result to individuals in the event of a breach, which
3 ultimately came to pass.

4 126. Defendant's various violations and its failure to comply with applicable laws and
5 regulations constitutes negligence *per se*.

6 127. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and
7 Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

8 **THIRD CAUSE OF ACTION**
9 **Breach of Implied Contract**
10 **(On Behalf of Plaintiff and the Class)**

11 128. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

12 129. Plaintiff and Class members were required to provide their PII/PHI to Defendant
13 as a condition of receiving employment provided by Defendant. Plaintiff and Class members
14 provided their PII/PHI to Defendant or its third-party agents in exchange for Defendant's
15 employment.

16 130. Plaintiff and Class members reasonably understood that a portion of the funds they
17 paid Defendant (or derived from their employment with Defendant) would be used to pay for
18 adequate cybersecurity measures.

19 131. Plaintiff and Class members reasonably understood that Defendant would use
20 adequate cybersecurity measures to protect the PII/PHI that they were required to provide based
21 on Defendant's duties under state and federal law and its internal policies.

22 132. Plaintiff and the Class members accepted Defendant's offers by disclosing their
23 PII/PHI to Defendant or its third-party agents in exchange for employment.

24 133. In turn, and through internal policies, Defendant agreed to protect and not disclose
25 the PII/PHI to unauthorized persons.

26 134. In its Privacy Policy, Defendant represented that they had a legal duty to protect
27 Plaintiff's and Class Member's PII/PHI.
28

1 135. Implicit in the parties' agreement was that Defendant would provide Plaintiff and
2 Class members with prompt and adequate notice of all unauthorized access and/or theft of their
3 PII/PHI.

4 136. After all, Plaintiff and Class members would not have entrusted their PII/PHI to
5 Defendant in the absence of such an agreement with Defendant.

6 137. Plaintiff and the Class fully performed their obligations under the implied
7 contracts with Defendant.

8 138. The covenant of good faith and fair dealing is an element of every contract. Thus,
9 parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair
10 dealing, in connection with executing contracts and discharging performance and other duties
11 according to their terms, means preserving the spirit—and not merely the letter—of the bargain.
12 In short, the parties to a contract are mutually obligated to comply with the substance of their
13 contract in addition to its form.

14 139. Subterfuge and evasion violate the duty of good faith in performance even when
15 an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And
16 fair dealing may require more than honesty.

17 140. Defendant materially breached the contracts it entered with Plaintiff and Class
18 members by:

- 19 a. failing to safeguard their information;
- 20 b. failing to notify them promptly of the intrusion into its computer systems
21 that compromised such information.
- 22 c. failing to comply with industry standards;
- 23 d. failing to comply with the legal obligations necessarily incorporated into
24 the agreements; and
- 25 e. failing to ensure the confidentiality and integrity of the electronic PII/PHI
26 that Defendant created, received, maintained, and transmitted.

27 141. In these and other ways, Defendant violated its duty of good faith and fair dealing.
28

1 142. Defendant's material breaches were the direct and proximate cause of Plaintiff's
2 and Class members' injuries (as detailed *supra*).

3 143. And, on information and belief, Plaintiff's PII/PHI has already been published—
4 or will be published imminently—by cybercriminals on the Dark Web.

5 144. Plaintiff and Class members performed as required under the relevant agreements,
6 or such performance was waived by Defendant's conduct.

7 **FOURTH CAUSE OF ACTION**
8 **Invasion of Privacy**
9 **(On Behalf of Plaintiff and the Class)**

10 145. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

11 146. Plaintiff and the Class had a legitimate expectation of privacy regarding their
12 highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this
13 information against disclosure to unauthorized third parties.

14 147. Defendant owed a duty to its current and former employees, including Plaintiff
15 and the Class, to keep this information confidential.

16 148. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class
17 members' PII/PHI is highly offensive to a reasonable person.

18 149. The intrusion was into a place or thing which was private and entitled to be private.
19 Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but did
20 so privately, with the intention that their information would be kept confidential and protected
21 from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such
22 information would be kept private and would not be disclosed without their authorization.

23 150. The Data Breach constitutes an intentional interference with Plaintiff's and the
24 Class's interest in solitude or seclusion, either as to their person or as to their private affairs or
25 concerns, of a kind that would be highly offensive to a reasonable person.

26 151. Defendant acted with a knowing state of mind when it permitted the Data Breach
27 because it knew its information security practices were inadequate.
28

1 152. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and
2 the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation
3 efforts.

4 153. Acting with knowledge, Defendant had notice and knew that its inadequate
5 cybersecurity practices would cause injury to Plaintiff and the Class.

6 154. As a proximate result of Defendant's acts and omissions, the private and sensitive
7 PII/PHI of Plaintiff and the Class were stolen by a third party and is now available for disclosure
8 and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as
9 detailed *supra*).

10 155. And, on information and belief, Plaintiff's PII/PHI has already been published—
11 or will be published imminently—by cybercriminals on the Dark Web.

12 156. Unless and until enjoined and restrained by order of this Court, Defendant's
13 wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class
14 since their PII/PHI are still maintained by Defendant with their inadequate cybersecurity system
15 and policies.

16 157. Plaintiff and the Class have no adequate remedy at law for the injuries relating to
17 Defendant's continued possession of their sensitive and confidential records. A judgment for
18 monetary damages will not end Defendant's inability to safeguard the PII/PHI of Plaintiff and the
19 Class.

20 158. In addition to injunctive relief, Plaintiff, on behalf of himself and the other Class
21 members, also seeks compensatory damages for Defendant's invasion of privacy, which includes
22 the value of the privacy interest invaded by Defendant, the costs of future monitoring of their
23 credit history for identity theft and fraud, plus prejudgment interest and costs.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

159. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

160. This claim is pleaded in the alternative to the breach of implied contract claim.

161. Plaintiff and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from using their (1) PII/PHI to facilitate employment, and (2) labor to generate revenue.

162. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members.

163. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

164. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII/PHI.

165. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

166. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' (1) PII/PHI and (2) employment because Defendant failed to adequately protect their PII/PHI.

167. Plaintiff and Class members have no adequate remedy at law.

168. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

SIXTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

169. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

170. Given the relationship between Defendant and Plaintiff and Class members, where Defendant became guardian of Plaintiff's and Class members' PII/PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' PII/PHI; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

171. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

172. Because of the highly sensitive nature of the PII/PHI, Plaintiff and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices.

173. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII/PHI.

174. Defendant also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

175. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

SEVENTH CAUSE OF ACTION
Violation of California's Unfair Competition Law (UCL)
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of Plaintiff and the Class)

176. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

1 177. Defendant engaged in unlawful and unfair business practices in violation of Cal.
2 Bus. & Prof. Code § 17200, *et seq.* which prohibits unlawful, unfair, or fraudulent business acts
3 or practices (“UCL”).

4 178. Defendant’s conduct is unlawful because it violates the California Consumer
5 Privacy Act of 2018, Civ. Code § 1798.100, *et seq.* (the “CCPA”) and other state data security
6 laws.

7 179. Defendant stored the PII/PHI of Plaintiff and the Class in its computer systems
8 and knew or should have known it did not employ reasonable, industry standard, and appropriate
9 security measures that complied with applicable regulations and that would have kept Plaintiff’s
10 and the Class’s PII/PHI secure to prevent the loss or misuse of that PII/PHI.

11 180. Defendant failed to disclose to Plaintiff and the Class that their PII/PHI was not
12 secure. However, Plaintiff and the Class were entitled to assume, and did assume, that Defendant
13 had secured their PII/PHI. At no time were Plaintiff and the Class on notice that their PII/PHI was
14 not secure, which Defendant had a duty to disclose.

15 181. Defendant also violated California Civil Code § 1798.150 by failing to implement
16 and maintain reasonable security procedures and practices, resulting in an unauthorized access
17 and exfiltration, theft, or disclosure of Plaintiff’s and the Class’s nonencrypted and nonredacted
18 PII/PHI.

19 182. Had Defendant complied with these requirements, Plaintiff and the Class would
20 not have suffered the damages related to the data breach.

21 183. Defendant’s conduct was unlawful, in that it violated the CCPA.

22 184. Defendant’s acts, omissions, and misrepresentations as alleged herein were
23 unlawful and in violation of, *inter alia*, Section 5(a) of the Federal Trade Commission Act.

24 185. Defendant’s conduct was also unfair, in that it violated a clear legislative policy in
25 favor of protecting consumers from data breaches.

26 186. Defendant’s conduct is an unfair business practice under the UCL because it was
27 immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct
28

1 includes employing unreasonable and inadequate data security despite its business model of
2 actively collecting PII/PHI.

3 187. Defendant also engaged in unfair business practices under the “tethering test.” Its
4 actions and omissions, as described above, violated fundamental public policies expressed by the
5 California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 (“The Legislature declares that . . . all
6 individuals have a right of privacy in information pertaining to them . . . The increasing use of
7 computers . . . has greatly magnified the potential risk to individual privacy that can occur from
8 the maintenance of personal information.”); Cal. Civ. Code § 1798.81.5(a) (“It is the intent of the
9 Legislature to ensure that personal information about California residents is protected.”); Cal.
10 Bus. & Prof. Code § 22578 (“It is the intent of the Legislature that this chapter [including the
11 Online Privacy Protection Act] is a matter of statewide concern.”). Defendant’s acts and
12 omissions thus amount to a violation of the law.

13 188. Instead, Defendant made the PII/PHI of Plaintiff and the Class accessible to
14 scammers, identity thieves, and other malicious actors, subjecting Plaintiff and the Class to an
15 impending risk of identity theft. Additionally, Defendant’s conduct was unfair under the UCL
16 because it violated the policies underlying the laws set out in the prior paragraph.

17 189. As a result of those unlawful and unfair business practices, Plaintiff and the Class
18 suffered an injury-in-fact and have lost money or property.

19 190. For one, on information and belief, Plaintiff’s and the Class’s stolen PII/PHI has
20 already been published—or will be published imminently—by cybercriminals on the dark web.

21 191. The injuries to Plaintiff and the Class greatly outweigh any alleged countervailing
22 benefit to consumers or competition under all of the circumstances.

23 192. There were reasonably available alternatives to further Defendant’s legitimate
24 business interests, other than the misconduct alleged in this complaint.

25 193. Therefore, Plaintiff and the Class are entitled to equitable relief, including
26 restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to
27 Defendant because of its unfair and improper business practices; a permanent injunction enjoining
28

1 Defendant's unlawful and unfair business activities; and any other equitable relief the Court
2 deems proper.

3 **EIGHTH CAUSE OF ACTION**
4 **Violations of the California Consumer Privacy Act ("CCPA")**
5 **Cal. Civ. Code § 1798.150**
6 **(On Behalf of Plaintiff and the Class)**

7 194. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

8 195. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to
9 implement and maintain reasonable security procedures and practices appropriate to the nature of
10 the information to protect the nonencrypted PII/PHI of Plaintiff and the Class. As a direct and
11 proximate result, Plaintiff's and the Class's nonencrypted and nonredacted PII/PHI was subject
12 to unauthorized access and exfiltration, theft, or disclosure.

13 196. Defendant is a "business" under the meaning of Civil Code § 1798.140 because
14 Defendant is a "corporation, association, or other legal entity that is organized or operated for the
15 profit or financial benefit of its shareholders or other owners" that "collects consumers' personal
16 information" and is active "in the State of California" and "had annual gross revenues in excess
17 of twenty-five million dollars (\$25,000,000) in the preceding calendar year." Civil Code §
18 1798.140(d).

19 197. Plaintiff and Class Members seek injunctive or other equitable relief to ensure
20 Defendant hereinafter adequately safeguards PII/PHI by implementing reasonable security
21 procedures and practices. Such relief is particularly important because Defendant continues to
22 hold PII/PHI, including Plaintiff's and Class members' PII/PHI. Plaintiff and Class members have
23 an interest in ensuring that their PII/PHI is reasonably protected, and Defendant has demonstrated
24 a pattern of failing to adequately safeguard this information.

25 198. Pursuant to California Civil Code § 1798.150(b), Plaintiff mailed a CCPA notice
26 letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that
27 Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and
28

1 Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff
 2 intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

3 199. As described herein, an actual controversy has arisen and now exists as to whether
 4 Defendant implemented and maintained reasonable security procedures and practices appropriate
 5 to the nature of the information so as to protect the personal information under the CCPA.

6 200. A judicial determination of this issue is necessary and appropriate at this time
 7 under the circumstances to prevent further data breaches by Defendant.

8 **TENTH CAUSE OF ACTION**
 9 **Declaratory Judgment**
 10 **(On Behalf of Plaintiff and the Class)**

11 201. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

12 202. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is
 13 authorized to enter a judgment declaring the rights and legal relations of the parties and to grant
 14 further necessary relief. The Court has broad authority to restrain acts, such as those alleged
 15 herein, which are tortious and unlawful.

16 203. In the fallout of the Data Breach, an actual controversy has arisen about
 17 Defendant's various duties to use reasonable data security. On information and belief, Plaintiff
 18 alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff
 19 and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

20 204. Given its authority under the Declaratory Judgment Act, this Court should enter a
 21 judgment declaring, among other things, the following:

- 22 a. Defendant owed—and continues to owe—a legal duty to use reasonable
 23 data security to secure the data entrusted to it;
- 24 b. Defendant has a duty to notify impacted individuals of the Data Breach
 25 under the common law and Section 5 of the FTC Act;
- 26 c. Defendant breached, and continues to breach, its duties by failing to use
 27 reasonable measures to the data entrusted to it; and
 28

1 d. Defendant breaches of its duties caused—and continues to cause—injuries
2 to Plaintiff and Class members.

3 205. The Court should also issue corresponding injunctive relief requiring Defendant
4 to use adequate security consistent with industry standards to protect the data entrusted to it.

5 206. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury
6 and lack an adequate legal remedy if Defendant experiences a second data breach.

7 207. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy
8 at law because many of the resulting injuries are not readily quantified in full and they will be
9 forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—
10 while warranted for out-of-pocket damages and other legally quantifiable and provable
11 damages—cannot cover the full extent of Plaintiff and Class members' injuries.

12 208. If an injunction is not issued, the resulting hardship to Plaintiff and Class members
13 far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

14 209. An injunction would benefit the public by preventing another data breach—thus
15 preventing further injuries to Plaintiff, Class members, and the public at large.

16 **PRAYER FOR RELIEF**

17 Plaintiff and Class members respectfully request judgment against Defendant and that the
18 Court enter an order:

- 19 A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class,
20 appointing Plaintiff as class representative, and appointing his counsel to represent
21 the Class;
- 22 B. Awarding declaratory and other equitable relief as necessary to protect the
23 interests of Plaintiff and the Class;
- 24 C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the
25 Class;
- 26 D. Enjoining Defendant from further unfair and/or deceptive practices;
- 27
- 28

- 1 E. Awarding Plaintiff and the Class damages including applicable compensatory,
2 exemplary, punitive damages, and statutory damages, as allowed by law;
3 F. Awarding restitution and damages to Plaintiff and the Class in an amount to be
4 determined at trial;
5 G. Awarding attorneys' fees and costs, as allowed by law;
6 H. Awarding prejudgment and post-judgment interest, as provided by law;
7 I. Granting Plaintiff and the Class leave to amend this complaint to conform to the
8 evidence produced at trial; and
9 J. Granting other relief that this Court finds appropriate.

10
11 **DEMAND FOR JURY TRIAL**

12 Plaintiff demands a jury trial for all claims so triable.

13
14 Dated: June 3, 2024

Respectfully Submitted,

15 By: /s/ Andrew G. Gunem
16 Andrew G. Gunem
17 STRAUSS BORRELLI PLLC
18 One Magnificent Mile
19 980 N Michigan Avenue, Suite 1610
20 Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
agunem@straussborrelli.com

21 *Attorneys for Plaintiff and the Proposed Class*
22
23
24
25
26
27
28